Market Guide for Network Access Control

Published 12 May 2020 - ID G00719265 - 30 min read

By Analysts John Watts, Lawrence Orans, Claudio Neiva

Initiatives:Infrastructure Security

Network access control vendors are expanding offerings to adjacent markets; however, most clients implement NAC for the most common use cases. Security and risk management leaders must focus on the basics of NAC implementations before moving to adjacent use cases to achieve success.

Overview

Key Findings

- Most organizations interested in network access control (NAC) are looking to establish security of devices and users accessing the network, driven primarily by audit findings and to some degree a zero trust network security strategy.

- NAC is a mature technology with both commercial and open-source solutions on the market, providing feature sets that satisfy most organizational needs.

- NAC vendors are differentiating by expanding solutions into adjacent markets, such as asset discovery and management, Internet of Things (IoT) security, zero trust network access (ZTNA) and enabling network segmentation.

- Smaller NAC vendors tend to have a regional presence, focus on midsize and smaller organizations, or primarily serve certain verticals such as education or hospitality.

Recommendations

Security and risk management leaders responsible for network and endpoint security should:

- Implement NAC solutions that integrate well with existing network infrastructure and security solutions to improve security incident response times and lower overall operating overhead for the NAC product itself.

- Focus primary evaluation criteria of NAC solutions on vendors’ abilities to align with an organization’s goals, such as discovery and device visibility, preconnect or postconnect authentication and ease of use, more than on detailed technical comparisons across solutions.

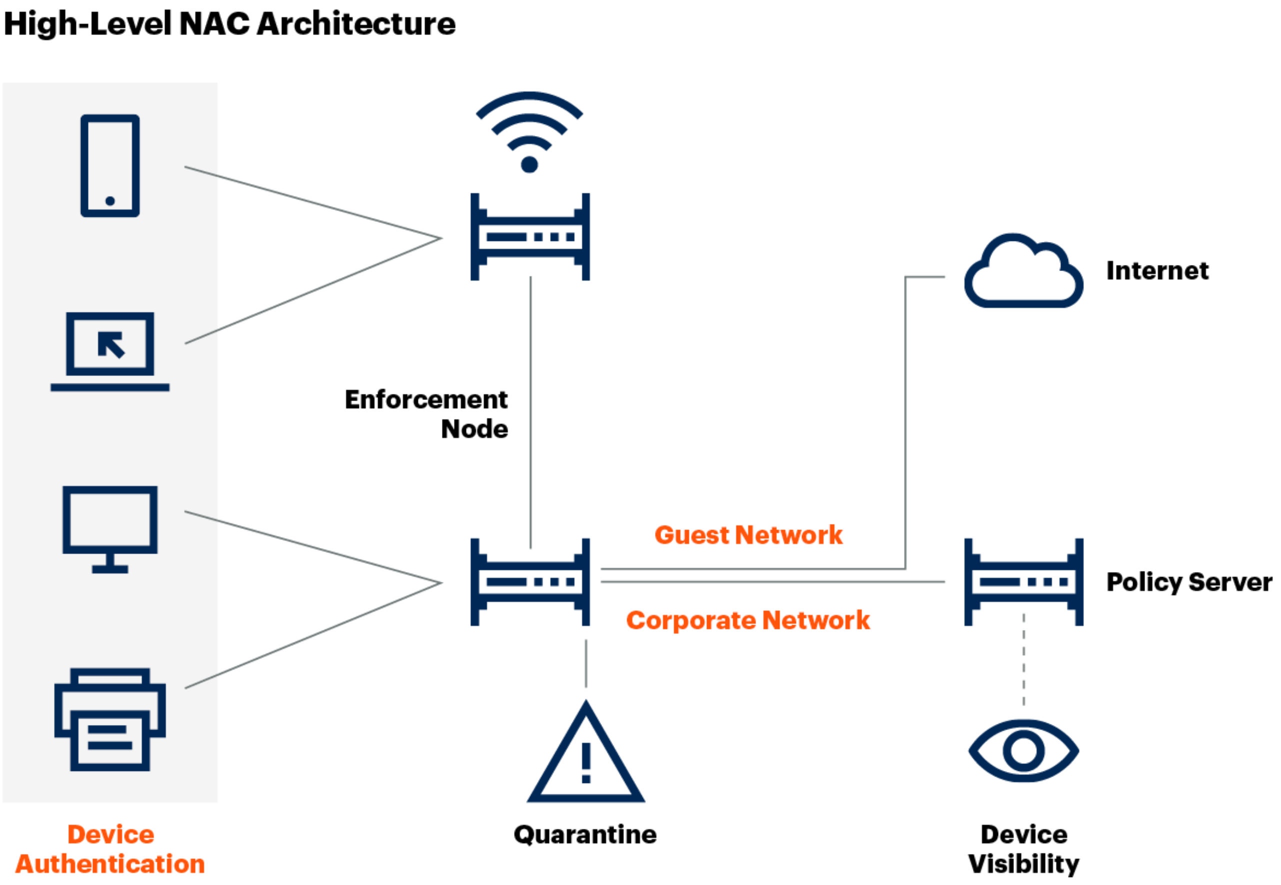
- Plan a multiphase implementation effort that requires commitment from multiple teams including executives, networking, endpoint, service desk and security teams — even for moderately complex organizations.

Market Definition

This document was revised on 14 May 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Gartner defines network access control as technologies that enable organizations to implement policies for controlling access to corporate infrastructure by both user-oriented devices and cyber physical devices such as IoT and operational technology (OT) devices. Policies may be based on authentication, endpoint configuration (posture) or users' role/identity. NAC can also implement postconnect policies based on integration with other security products. For example, NAC could enforce a policy to contain the endpoint based on an alert from a security information and event management (SIEM) tool (Figure 1).

Figure 1: NAC High-Level Architecture



Source: Gartner

719265_C

However, organizations looking to evaluate NAC on technical merits should start with capabilities detailed in the "Toolkit: Sample RFP for Network Access Control." At a high level, those aspects include:

- Policy server
- Visibility and reporting

- Device security posture check
- Guest management and identity
- Integration with other solutions
- Total cost of ownership (TCO)

Market Description

The commercial NAC providers can be grouped into two categories, pure-play NAC vendors and network infrastructure vendors.

Pure-Play NAC Vendors

Pure-play NAC vendors have a dedicated solution that supports heterogeneous networking devices. Both open source with paid-for support and commercial products are available. Due to their focus on multivendor support and integration, pure-play NAC solutions integrate with a wide range of security products, such as firewalls, endpoint protection platforms and others. However, pure-play NAC vendors stand out for their ease of use by offering authentication alternatives to the 802.1X protocol and Media Access Control (MAC) authentication. Therefore, the main advantages of this type of provider are the ease of deployment, ease of use, ability to support nearly any hardware, and flexible methods of policy enforcement in the network infrastructure.

Network Infrastructure Vendors

The NAC solutions of network infrastructure providers typically utilize a Remote Authentication Dial-In User Service (RADIUS)-based method to control access to the network by devices in combination with user access control based on identity (authentication) and MAC authentication. 802.1X is the preferred method of implementation. The main advantages of choosing this type of vendor are vendor consolidation and tight integration with existing vendor networking products and components.

Market Direction

The NAC market continues to primarily provide visibility and control for access to an organization's on-premises IT infrastructure. However, cyber-physical system security capabilities for IoT and OT devices continue to improve, and several alternatives to NAC exist in the market today depending on the capabilities required.

Cyber-Physical Systems

NAC vendors continue to acquire or partner with vendors focused on cyber-physical system security, especially in verticals sensitive to cyber-physical system security risks, such as healthcare, critical infrastructure and manufacturing. NAC vendors discover IoT devices by scanning the network infrastructure regardless of whether it is wired or wireless to provide security leaders the visibility to define what policy would be appropriate for each use case. One example is separating OT devices from IT infrastructure by applying segmentation to the network devices through access control list (ACL) and virtual LAN (VLAN) assignments. IoT devices (such as DVRs, CCTV and web cameras), smart lighting systems, building automation and facilities management systems all may be partially or entirely connected to corporate data networks in the organization without IT awareness.

Alternatives to NAC Providers

NAC uniquely satisfies multiple security use cases for device security on the corporate network. However, depending on the organization's need, a combination of different solutions in adjacent markets might provide the same features and benefits as an NAC provider. It is important for SRM leaders to understand the goal of their NAC implementation to determine if an NAC provider is required or if existing solutions satisfy their requirements.

Many cyber-physical system security vendors exist and often focus on a specific vertical industry. They do not fulfill all the common use cases for NAC, such as corporate and guest laptop security, and, therefore, may only be a partial solution. More often, these solutions are integrated with an NAC solution or existing network infrastructure to improve device visibility and control where an agent cannot be deployed. For more details see "Emerging Technology Analysis: Cyber-Physical Systems Security Is an Opportunity for Security Product Managers." For a list of IoT- and OT-specific security vendors, see "Market Guide for Operational Technology Security."

Zero trust network access is a new category of solutions that also has some overlap with NAC functionality and is related to a longer-term secure access service edge (SASE) trend (see "The Future of Network Security Is in the Cloud"). However, it is mostly focused on remote access use cases for laptops and mobile devices and not for local network device security. Most ZTNA vendors do not handle asset discovery, headless device access nor on-premises guest device wireless access security. ZTNA vendors can authenticate users and devices, provide some endpoint posture assessments, and control access to applications, accomplishing some of the security goals for NAC. Some NAC vendors also offer ZTNA products in addition to their NAC offerings, which may be integrated or completely independent. For more details and a list of vendors, see "Market Guide for Zero Trust Network Access."

IT asset management solutions can provide device visibility and inventory. Many of these solutions are aligned to the IT service management (ITSM) space and implemented as part of a service asset and configuration management (SACM) program to discover and report on assets on the network. However, they generally lack the enforcement capabilities of an NAC. Some NAC vendors support bidirectional integration with popular platforms to maintain a more accurate list of devices between the two systems. For more details and a list of ITSM vendors, see "Magic Quadrant for IT Service Management Tools."

Wireless access is considered more vulnerable than wired access due to the wide array of devices that can connect over wireless, especially outside of physical security control boundaries. Wireless access point (WAP) solutions often provide security, such as user and device authentication, bring your own device (BYOD) and guest management in addition to wireless intrusion prevention systems (WIPSs), to prevent unauthorized access. Network infrastructure vendors offer WAP security as well as NAC, while others may only focus on WAP solutions. For companies looking only for wireless security, these solutions provide many of the same benefits of an NAC. However, they may not provide a full device inventory, endpoint posture assessments or security for wired networks. For more details and a list of LAN access infrastructure options, see "Magic Quadrant for Wired and Wireless LAN Access Infrastructure."

Unified endpoint management (UEM) vendors can often provide per-app VPN connections as well as endpoint security posture checks. Many of these vendors can control remote access as well as local access to applications as long as the applications are published, managed, and accessed exclusively through their solution. UEM products could be used in replacement for corporate-owned or BYOD use cases for NAC as they require endpoint enrollment to work. These solutions do not work if there are guest device portal needs or the need to manage headless devices such as printers or cameras in the network. Nor do they protect the core wired LAN from unauthorized access by third parties. The most common scenario is for NAC vendors to integrate to UEM vendors for a simple check for enrollment and compliance before allowing access to the network. For more details on UEM vendors, see "Magic Quadrant for Unified Endpoint Management Tools."

Market Analysis

Gartner sees the NAC market as mature and growing slowly. In June 2020, Gartner will start to report network access control (NAC) in its forecast and revenue share by vendor in its Market Share reports (see "Update: Gartner to Revise Its Enterprise Network Equipment Forecast and Market Share Coverage"). There are few new entrants and some consolidation through acquisition seen in the market over the past few years. The drivers considered by clients when implementing an NAC solution are:

- Preconnect or postconnect authentication approach. The preconnect authentication can be thought of as a "guilty until proven innocent" model ("default deny"); whereas postconnect authentication can be considered as an "innocent until proven guilty" model ("default allow").

- Visibility into on-premises infrastructure-connected devices with the goal of implementing access policies. This includes commonly used devices (such as a workstation, laptop, printer, IP phone, IP camera, access points, and IoT devices like OT devices, medical devices and building automation). Often, this is driven by audit findings or an overall security strategy to require authentication of all devices to the network.

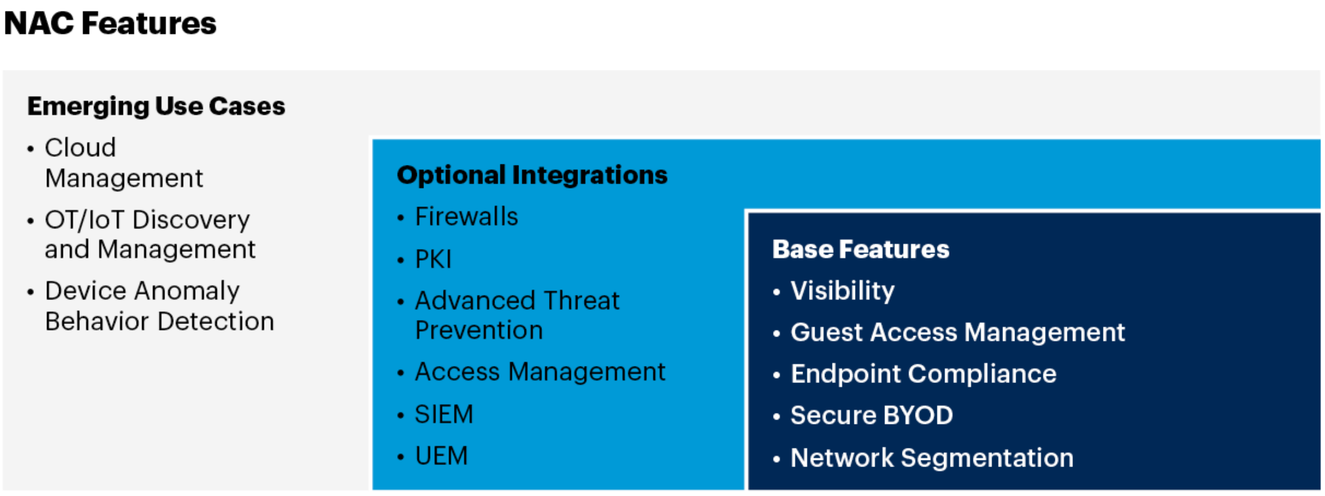
- Management of corporate network access for different types of users and devices, such as employees, contractors, consultants and guests, using either corporate-owned or user-provided endpoints.

- Ability to analyze compliance with a minimum security posture at the endpoint and provision of a quarantine network for devices not in compliance. For example, verify that the endpoint has an endpoint protection platform (EPP) installed, and that most critical security patches are installed. If not, that device is only allowed access to a quarantine VLAN until those items are remediated.

- Interoperability with other security solutions. Integration with other solutions can happen in two ways: customization through open APIs or the use of built-in integration. NAC solutions are increasingly adding an anomaly detection capability to detect infected endpoints and MAC spoofing attempts on the network. Integration with other security tools enables better overall security context for an organization, which can be used to automatically respond to infected endpoints to quarantine them and prevent the spread of malware.

NAC continues to be primarily an on-premises deployment requiring hardware or virtual appliances, but increasingly vendors have extended management to the cloud or provided cloud-based RADIUS services. These offerings provide a way to consolidate management of distributed NAC implementations through the cloud rather than over private networks. Some solutions integrate with additional products or provide brokers deployed to help bridge on-premises networks and cloud management functions (see Figure 2).

Figure 2: NAC Features



Source: Gartner

719265_C

Representative Vendors

Market Introduction

The vendors in this Market Guide offer at least the capabilities listed in the Market Definition section.

Table 1: Representative Vendors in Network Access Control

Vendor ↓	*Product, Service or Solution Name* ↓
ActZero-IntelliGO Networks	IntelliGO MDR Platform
Auconet	Business Infrastructure Control Solution (BICS)
Cisco	Cisco Identity Services Engine (ISE)
CommScope	Cloudpath Enrollment System
Extreme	ExtremeControl ExtremeCloud A3
Forescout Technologies	Forescout Platform
Fortinet	FortiNAC
Genians	Genian NAC
Hewlett Packard Enterprise (HPE)-Aruba	Aruba ClearPass
InfoExpress	Easy NAC CGX
Inverse	PacketFence
OPSWAT-Impulse	SafeConnect
macmon secure	macmon NAC
Netshield	Netshield
Open Cloud Factory	OpenNAC Enterprise
Portnox	CLEAR CORE

Vendor ↓	*Product, Service or Solution Name* ↓
Pulse Secure	Pulse Policy Secure (PPS)

Source: Gartner (May 2020)

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Vendor Profiles

ActZero-IntelliGO

Founded in 2005, IntelliGO Networks is a privately held company owned by ActZero, a U.S.-based artificial intelligence (AI) firm. IntelliGO provides a service for managed detection and response for small and midsize businesses (SMBs) based on the IntelliGO MDR platform. The RADIUS-based IntelliGO MDR platform supports network control through IntelliGO agents and virtual appliances. The service scales using cloud-based management infrastructure to support both agent and agentless enforcement techniques.

IntelliGO MDR platform promotes NAC as a managed service with monitoring and response from a threat hunting team assisted through AI techniques. IntelliGO MDR platform can ingest data from security tools such as firewalls and servers. In addition, it has vulnerability scanning engines and collects raw events to measure security posture against threat intelligence feeds and supports threat hunting use cases. Updates in the IntelliGO MDR Platform since 2018 include agentless control through SSH enforcement and quarantine of off-network endpoints using agents. In addition, enhancements in audit logging for analytics, artificial intelligence and automation (AAA), endpoint detection and response (EDR), vulnerability assessment (VA) scans and hygiene (posture).

Auconet

Auconet is a privately held company with headquarters in Germany and sales/consulting in Western/Eastern Europe and North America. It has been delivering NAC solutions since 2005. The vendor has integrated NAC security and network troubleshooting capabilities into one solution for operations and security use cases for heterogeneous networks. Auconet works directly with global enterprises and with managed security service providers (MSSPs) offering large-scale, multitenant, managed NAC services.

The Auconet Business Infrastructure Control Solution (BICS) is deployed most commonly as an agentless solution, using Layer 2 MAC-based authentication, in addition to its RADIUS- based policy server, which supports native 802.1X supplicants embedded in multiple OSs. BICS is available as a hardware appliance, a virtual appliance or SaaS. Auconet also offers an optional permanent agent on Windows, UNIX/Linux platforms and macOS. Since 2018, Auconet implemented two major features to improve user experience through an HTML5-based web interface and control for VLAN/ports in emergency use cases. Also, endpoint monitoring was enhanced by the release of Auconet's own agents and by increased location/visibility of devices through Wi-F- based on expansion of supported Wi-Fi vendors. In addition, for bidirectional integrations Auconet expanded REST API integration capabilities.

Cisco

Cisco's Identity Services Engine (ISE) is based on the IEEE 802.1X standard. ISE is available in hardware appliances and as a virtual server. ISE is one of the most popular NAC solutions in the market. Through its pxGrid framework, Cisco integrates with its own security products and with third-party solutions. pxGrid enables ISE to share alerts and contextual information between those other security products to increase visibility and enable informed policy decisions. Cisco packages its NAC agent with its AnyConnect endpoint bundle.

ISE can function as a stand-alone NAC or as part of the software-defined access (SDA) solution through its integration with the Cisco DNA Center for automated and unified policy enforcement. In 2019, Cisco made several improvements to ISE. It increased its scalability (by introducing new appliances) to support up to two million endpoints. It improved some usability features, including simplifying the guest user experience and easing the administration of some ISE configurations. Also in 2019, Cisco acquired Sentryo, a company that delivered NAC-like functionality for IoT/OT devices. Cisco has integrated Sentryo into the ISE solution rebranded as Cisco Cyber Vision.

CommScope

In 2015, Ruckus Wireless acquired Cloudpath Networks, known primarily for its Wi-Fi onboarding products. In 2017, ARRIS acquired Ruckus; and, in 2019, CommScope acquired ARRIS. CommScope now offers Cloudpath Enrollment System, which is an enhanced version of the original Cloudpath Networks solution. Cloudpath Enrollment System supports a variety of network authentication protocols including 802.1X for both wired and wireless networks. The solution provides NAC functionality for guests, BYOD users, and IT-owned and managed devices.

Cloudpath Enrollment System is available as a virtual machine for on-site deployment or consumed as a SaaS. CommScope works well with its existing Ruckus Wireless customers as well as customers with standards-based networking equipment. Cloudpath Enrollment System has been popular for small to midsize business as well as in verticals such as education and hospitality.

Extreme

Extreme is based in San Jose, California. In addition to ExtremeControl (NAC), Extreme offers other security products (such as AirDefense from the Zebra acquisition, ExtremeGuest for guest wireless security and analytics, and Extreme Defender for IoT, which secures IoT devices when they connect to the network). Extreme acquired Aerohive Networks in August, 2019 and now offers a cloud managed NAC (ExtremeCloud A3) in addition to its on-premises product (ExtremeControl). The primary use case for NAC is for ExtremeSwitching and WLAN customers, although the solution can support non-Extreme environments.

Extreme's NAC offerings are AAA and RADIUS-based solutions that are available in multiple delivery models. Extreme's tight integration of its NAC solution with its unified wired/wireless product family enables granular policy enforcement. Policies may permit, deny, apply quality of service (QoS), rate limit and implement other controls to traffic based on user identity, time, location, end system and user groups. In addition, Extreme offers virtual machine (VM) management by applying policy on virtual switch (vSwitch) and physical switches to manage VM access through VMware and OpenStack integration. In 2019, Extreme released the ExtremeCloud A3 cloud-managed NAC solution (based on technology from the Aerohive Networks acquisition). It also enhanced its ExtremeControl NAC with customizable workflows and onboarding for non-IT devices, expanded its endpoint security ecosystem, and added comprehensive guest analytics.

Forescout Technologies

Forescout, based in San Jose, California, began trading as a public company in October 2017 and announced an intent to become a private company in February 2020. The company sells its Forescout Platform (formerly known as CounterACT) for device visibility and control use cases. It is one of the most popular NAC solutions in the market. The Forescout Platform consists of multiple products: eyeSight, eyeControl, eyeSegment and eyeExtend. Forescout's platform can be deployed on hardware, virtual appliances and public cloud for midsize to large deployments.

Although Forescout offers optional agents, its agentless approach performs a security posture assessment for Windows, macOS, Linux and IoT devices. Forescout provides a series of eyeExtend modules and crowdsourced apps that share contextual information and orchestrate workflows with third-party products. Via these modules, eyeControl can be configured to automatically enforce policy (for example, remove an endpoint from the network) in response to alerts from advanced threat detection (ATD), VA, EDR, SIEM and other third-party products. In 2018, Forescout acquired SecurityMatters and now provides its integrated SilentDefense solution to improve overall visibility, risk monitoring and response capabilities for the OT stack. It also announced a partnership with Medigate for medical device visibility and control, and released the eyeSegment product for network segmentation across multivendor enforcement technologies and network domains.

Fortinet

In June 2018, Fortinet acquired Bradford Networks, one of the earliest NAC vendors. Fortinet has rebranded the solution as FortiNAC, and it is available as hardware, virtual appliances or in the public cloud. Bradford Networks had a relatively low profile in the market, but since the acquisition, Gartner clients have been adding the solution to their "shortlists" more often, especially if they are existing Fortinet customers. FortiNAC's API support has enabled it to partner with many other third-party solutions to share contextual information and configure network devices. FortiNAC supports the Open Network Video Interface Forum (ONVIF) standard that was created to help IP products within video surveillance and other physical security areas communicate with each other. FortiNAC supports the IEEE 802.1X standard, although it is not reliant on it for discovery or enforcement.

In 2019, FortiNAC added the ability to push endpoint and network infrastructure device information to FortiAnalyzer for reporting. Fortinet also added profiling capabilities with secure Windows Management Instrumentation (WMI), secure Windows Remote Management (WinRM), Microsoft Intune, G Suite, and passive traffic scanning leveraging FortiGate NGFWs as traffic sensors. The traffic scanning for identification enables anomaly detection for traffic patterns.

Genians

Genians was founded in 2005, with its headquarters in South Korea and a global business office in Boston, Massachusetts. Genians' flagship solution, Genian NAC, is a sensor-based NAC solution that can host its management/policy component in the cloud or on-premises. Genian NAC stands out for its device detection capabilities through its Device Platform Intelligence (DPI) feature, which provides visibility by adding business context information (such as a device's end of life [EOL]/end of support [EOS] status, manufacture or vendor viability). Genian NAC monitors the life cycle of all IP-enabled devices based on Layer 2/Layer 3 protocols and other sources of information to increment the device profiling. The database passes to a DPI cloud for profile validation and shares new profiles with other Genians customers.

For customers that still need to keep fixed IP addresses on their devices for any reason, Genians maintains a complete mapping of devices and IP addresses being used to avoid problems related to two devices using the same IP address. Also, Genian NAC provides access control using ARP poisoning, TCP reset by switched port analyzer (SPAN) port, RADIUS/DHCP server and agents. Genian NAC also integrates with a number of IT security and business solutions for unified policy enforcement. In 2019, Genians added IPv6 support, SAML support for user authentication, "Time-Based Security TAGs," simplified 802.1X wired connection management, a dissolvable agent, and TACACS+ support among other NAC improvements.

Hewlett Packard Enterprise-Aruba

Hewlett Packard Enterprise (HPE) offers the Aruba ClearPass suite of network access solutions including Aruba ClearPass Device Insight and Aruba ClearPass Policy Manager. ClearPass Device Insight provides enhanced visibility based on AI-powered capabilities to perform automatic classification of unknown devices based on DPI-based discovery and profiling of devices. Aruba ClearPass Policy Manager offers enforcement and role-based access control based on RADIUS and non-RADIUS for user, server and OT/IoT devices options as well as TACACS+ for device management authentication. Deployment options include hardware and virtual appliances including support for Amazon Web Services (AWS).

ClearPass add-on capabilities include BYOD, device onboarding (ClearPass Onboard) and endpoint posture assessments (ClearPass OnGuard) with options for agentless, persistent or dissolvable agents. Third-party products have been integrated and validated using ClearPass Exchange, including firewalls, UEM and SIEM — via REST-based APIs, syslog messaging and RADIUS proxy functions. The ClearPass suite also includes embedded enforcement through integration with the Aruba Policy Enforcement Firewall, enabling dynamic segmentation to control access from wired, wireless and WAN connections applied with the same role and policy.

InfoExpress

InfoExpress is a privately held company, based in Santa Clara, California, focused on providing two NAC solutions. The Easy NAC solution uses appliances and inexpensive extenders to quarantine devices for highly distributed organizations without agents or network changes. The CGX solution offers multiple enforcement options for more complex networks, including RADIUS for 802.1X, in-line (typically used for VPN implementations), and agent-based Dynamic NAC (DNAC).

Both solutions include hardware or a virtual appliance option, and support Windows, macOS, and Linux agents. The NAC solutions correlate data from multiple sources, such as Active Directory, enterprise servers, syslog, Nmap, mobile device management (MDM) and agents to support NAC policies. For example, if a mobile device is detected with malware or reported as stolen and reappears on the network, the solutions will quarantine the device and notify administrators.

Inverse

Founded in 2008, Inverse is a privately held company based in Montreal, Quebec. Inverse develops the PacketFence NAC solution, which is completely free and open source. PacketFence is a RADIUS-based solution, and Inverse delivers consulting services and product support for the software.

PacketFence includes a captive portal for registration and remediation. It uses Fingerbank to leverage profiling capability. The Fingerbank solution is a set of device fingerprints that identifies endpoints connected to the network infrastructure. Inverse provides advanced auditing capabilities to PacketFence and a cloud version of PacketFence for the MSSP use case. Updates in PacketFence include an enhanced GUI interface along with public-key infrastructure (PKI), which allow PacketFence to provide native EAP-TLS support by its own certificate authority (CA). In addition, its network anomaly detection capabilities inspect network traffic searching for malicious behavior from endpoints. New supported firewalls for single sign-on include firewalls like those from Family Zone and Smoothwall, and the Rocket Appliance from Lightspeed Systems. VPN support is also an update (Cisco and Fortinet) to maintain control over remote users.

macmon secure

Macmon secure was founded in 2003 in Berlin, Germany with a focus on NAC in the European market. In 2018, macmon released version 5 of its NAC engine, which was completely redesigned for performance and scalability and has Common Criteria (EAL2+) certification. Macmon is based on SNMP and 802.1X. It includes support for guest management as well. Macmon offers topology mapping, endpoint device security, integrated RADIUS, VLAN management and guest services as part of its Network Bundle. The Premium Bundle includes compliance reporting and management, while additional add-on modules include the Past Viewer to enable forensic analysis of endpoint authentication and access events, Switch Viewer for assessing switch health across a network, and scalability modules.

Macmon focuses its NAC on simplicity and ease of use, particularly for SMBs and large European organizations with heterogeneous environments. Macmon supports integrations with technology partners such as Barracuda, Check Point Software Technologies, FireEye, F-Secure, Greenbone Networks, Sophos and others. In 2019, macmon released a cloud-based appliance, a REST API for additional third-party tool integrations, and an expanded set of automated rules generated based on initial discovery for switch configuration and RADIUS.

Netshield

Netshield offers a small-business-focused solution with monthly subscription and management options optimized for MSSPs. Targeting networks up to 4,000 assets, Netshield can be deployed virtually or via a hardware appliance. It is a non-in-line solution featuring agentless endpoint discovery to ensure instant identification of all network devices, including IoT and BYOD.

Beyond asset detection, devices that are not trusted, or those attempting to contact known malware or phishing sites are blocked using an ARP poison methodology. Additionally, switch ports can be shut off or devices moved to a quarantine VLAN via SmartSwitch integration. Netshield also has an onboard auditing engine to identify common vulnerabilities and exposures (CVE). Upon successful deployment and auditing, Netshield offers the first of its kind of cyberinsurance for U.S. customers with coverage up to $250,000 at no extra cost to the customer.

Updates from Netshield include a set of capabilities to make its solution easier to use, such as integration Active Directory, certification generation and global asset trusting. For security capabilities, Netshield included integration with SIEM, AI and machine learning solutions.

Open Cloud Factory

Based in Spain, Open Cloud Factory (OCF) is a pure-play NAC vendor focusing on both IT and OT environments. It targets midsize businesses, mostly in Europe and Latin America. Its OpenNAC Enterprise solution is offered as a virtual appliance hosted on-premises, in the public cloud or as a hybrid cloud. The core policy engine is based on 802.1X, although sensors can be implemented to provide passive asset discovery. OpenNAC Enterprise is certified by CCN-CERT, the Spanish National Cryptologic Center. The solution integrates with third-party security offerings such as SIEM, next-generation firewall (NGFW) and MDM through RESTful APIs.

The modular design of OpenNAC Enterprise allows organizations the flexibility to pay only for the functionality that they require. The solution includes seven modules: Visibility, Secure BYOD Adoption, Compliance, Network Segmentation, UniversalNetwork Access Control, Secure Remote Access and Guest Access Control. For the authentication process, it can integrate with multiple LDAPs and directories, and it may also include a second authentication factor using Google

Authenticator or Mobile Connect. In 2019, the company partnered with managed service providers (MSPs) to deliver NAC as a service.

OPSWAT-Impulse

San Francisco-based OPSWAT was founded in 2002 focusing on protecting critical infrastructure. OPSWAT offers multiple security offerings including MetaAccess for secure cloud access protection and MetaDefender for advanced threat prevention. In 2019, OPSWAT acquired Impulse to add the SafeConnect NAC and SafeConnect Software-Defined Perimeter (SDP) products to its existing security portfolio. OPSWAT delivers the SafeConnect NAC solution as a cloud-managed service, which includes system monitoring, problem determination and resolution, daily updates to device type, antivirus and OS profiling recognition, and remote backup of policy configuration data. All OPSWAT NAC products can be implemented as a virtual or cloud instance.

SafeConnect offers 802.1X and non-802.1X RADIUS-based policy enforcement options at a Layer 2 or Layer 3 enforcement approach that eliminates the need to integrate with Layer 2 LAN switches. SafeConnect's Network Security Orchestration feature correlates device type, user identity, location and ownership information, and shares contextual data to multiple third-party security platforms (such as VMware AirWatch, RSA, Palo Alto Networks, SonicWall, Fortinet, IBM QRadar and Splunk). This enables identity/role-based policies and security assessment analytics. Recent updates to SafeConnect include expansion of EPP and threat detection vendor integrations, expanded network vendor support, device fingerprinting improvements, and expanded IoT visibility and enforcement.

Portnox

Portnox is a pure-play NAC vendor that operates mainly in the Americas and EMEA and that typically targets midsize to large enterprises. The company offers two NAC solutions: Portnox CORE and Portnox CLEAR.

Portnox CORE is an on-premises solution implemented via software or virtual appliances as an agentless solution based on endpoint discovery. When Portnox CORE detects that a device has connected to the network, it checks the device's risk posture and applies the appropriate policy to the network access point (for example, LAN switch or wireless AP). Portnox CORE can also extend access control capabilities to IoT devices.

Portnox CLEAR is a cloud-delivered NAC-as-a-service offering with foundational technology based on 802.1X and a RADIUS server hosted in the cloud. Portnox CLEAR offers integrations with cloud authentication directories such as Microsoft Azure, G Suite and Okta. It also includes a self-enrollment onboarding portal (agentless) or a dedicated agent supporting iOS, Android, Windows, Linux and macOS devices. Through the use of dynamic policies, Portnox CLEAR allows organizations to profile and authenticate connected inventory and its owners (managed devices, IoT or BYOD) and to authorize access to networks or subset VLANs. It continuously assesses endpoint risk posture, and proactively remediate issues to keep devices in-line with internal compliance policies — across all access layers (wired, Wi-Fi and remote). In 2019, Portnox strengthened its support for its MSP partners with the release of a multitenant, self-service portal for MSPs on Portnox CLEAR.

Pulse Secure

Pulse Secure was created in 2014 when private equity firm Siris Capital acquired the Junos Pulse product line from Juniper. In addition to its NAC solution, Policy Secure, Pulse Secure offers its Pulse Access Suite of integrated VPN, SDP and application delivery, and a mobile security solution. The Pulse Policy Secure NAC solution is RADIUS-based inclusive of 802.1X, MAC authentication, TNC, SNMP and other standards. It is available as a family of hardware and virtual appliances. Pulse Policy Secure supports integrated NAC, SDP and VPN access in a heterogeneous network infrastructure.

Pulse Secure works with a broad range of security and network products and has furthered its integrations with other vendors such as Cisco, HP, Huawei, Juniper, Palo Alto Networks, Fortinet, Check Point Software Technologies, Splunk and IBM QRadar among others. Pulse Secure offers a central management, including one agent for its portfolio (VPN, SDP, NAC and mobile management) and enhancement in the profiling feature. Recent updates for Pulse Secure include user and entity behavior analytics (UEBA) anomaly detection, alert-based integration with Nozomi Networks for OT threat detection and response, agentless profiling, improved scale and load balancing, and support for hosting Pulse Policy Secure in Azure and AWS.

Market Recommendations

Organizations should focus on total implementation cost, alignment with organization type (size and industry vertical) and integration with existing infrastructure vendors to differentiate solutions. Most organizations only need to implement a single NAC solution and therefore should seek to consolidate if multiple NAC solutions exist within their environment. Multiple NAC solutions generally occur through M&A activities or by way of complex organizations making independent buying decisions. Given the range of solutions in the marketplace, we recommend that you:

- Focus on vendors that target organizations of your size and complexity and, in some instances, industry vertical or region. Because NAC is a mature market, many vendors are clearly aligned regarding SMB and large-enterprise opportunities or specialize in certain industry verticals and regions such as Europe and Southeast Asia.

- Align NAC projects with any zero trust security architecture initiative as NAC can be a primary means to achieve a default deny approach for devices connected to internal networks.

- Perform an initial network inventory before selecting an NAC vendor. This will influence your decision based on the capabilities of your network switches and routers, as well as help with budgeting since many NAC vendors license based on the number of IP addresses protected.

- Determine which UEM solutions are already installed on the network to identify providers that have direct integration with existing UEM solutions.

- Implement NAC to deliver visibility (for example, which devices are connected to your network) and control (allow or deny access) over your corporate network. Integrate with existing asset management solutions bidirectionally to help maintain an accurate list of devices connected to the organization.

- Use the postconnect functionality of your NAC solution. Most NAC products integrate with multiple security products. Configure NAC to automatically enforce policy when your threat detection solution (for example, network sandbox) alerts that an endpoint has been compromised. NAC can automatically remove the endpoint from the network, or it can enforce another policy that limits the endpoint's ability to communicate externally.

Clients should evaluate which security solutions the organization is using to see if such solutions exist in the list of built-in integration from the NAC vendor. This simplifies integration rather than having to "roll your own" integrations using available APIs. In addition, future security roadmaps may dictate the deployment of adjacent features such as VPN or ZTNA solutions, which may influence the choice of NAC provider to combine both remote and on-premises device posturing and control.

Acronym Key and Glossary Terms

Zero trust network access (ZTNA)	Products that create an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access.
Cyber-physical systems	Engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans) and enable safe, real-time, secure, reliable, resilient and adaptable performance.
Unified endpoint management (UEM)	A set of offerings that comprise mobile device management (MDM), modern management of traditional endpoints (PCs and Mac) and integration with client management tools (CMTs) and processes.

Note 1
Representative Vendor Selection

The vendors listed in this market guide are representative of the network access control market. We did not include vendors where the NAC solution is sold as a feature of other products.

Document Revision History

Market Guide for Network Access Control - 31 July 2018

Market Guide for Network Access Control - 9 May 2017

Market Guide for Network Access Control - 7 March 2016

Recommended by the Authors

Toolkit: Sample RFP for Network Access Control

How to Implement Network Access Control in Three Phases

How to Secure the Enterprise Against the Internet of Things Onslaught

Recommended For You

Gartner Peer Insights ‘Voice of the Customer’: Network Firewalls

Critical Capabilities for Network Firewalls

Magic Quadrant for Network Firewalls

How to Implement Network Access Control in Three Phases

Protecting Against ‘Living Off the Land’ Attacks